Constructions and Bounds for Visual Cryptography*

Giuseppe Ateniese[1], Carlo Blundo[1], Alfredo De Santis[1], and Douglas R. Stinson[2]

[1] Dipartimento di Informatica ed Applicazioni,
Università di Salerno, 84081 Baronissi (SA), Italy

[2] Department of Computer Science and Engineering
and Center for Communication and Information Science
University of Nebraska-Lincoln, Lincoln NE 68588, USA

Abstract. A visual cryptography scheme for a set $\mathcal{P}$ of n participants is a method to encode a secret image SI into n images in such a way that any participant in $\mathcal{P}$ receives one image and only qualified subsets of participants can "visually" recover the secret image, but non-qualified sets of participants have no information, in an information theoretical sense, on SI. A "visual" recover for a set $X \subseteq \mathcal{P}$ consists of stacking together the images associated to participants in X. The participants in a qualified set X will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation.

In this paper we propose two techniques to construct visual cryptography schemes for any access structure. We analyze the structure of visual cryptography schemes and we prove bounds on the size of the image distributed to the participants in the scheme. We provide a novel technique to realize k out of n visual cryptography schemes. Finally, we consider graph-based access structures, that is access structures in which any qualified set of participants contains at least an edge of a given graph whose vertices represent the participants of the scheme. Our constructions for 2 out of n visual cryptography schemes are the best possible with respect to pixel expansion and relative difference.

1 Introduction

A visual cryptography scheme for a set $\mathcal{P}$ of n participants is a method to encode a secret image SI into n images in such a way that any participant in $\mathcal{P}$ receives one image and only qualified subsets of participants can "visually" recover the secret image, but non-qualified sets of participants have no information, in an information theoretical sense, on SI. A "visual" recover for a set $X \subseteq \mathcal{P}$ consists of stacking together the images associated to participants in X. The participants

* Research of C. Blundo and A. De Santis is partially supported by Italian Ministry of University and Research (M.U.R.S.T.) and by National Council for Research (C.N.R.). Research of D. R. Stinson is supported by NSF grant CCR-9402141.

in a qualified set X will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation.

The best way to understand visual cryptography is by resorting to an example. Suppose that there are 4 participants, that is $\mathcal{P} = \{1,2,3,4\}$ and that the qualified sets are all subsets of $\mathcal{P}$ containing at least one of the following three sets $\{1,2\}$, $\{2,3\}$, and $\{3,4\}$, that is the family of qualified sets is $\mathcal{A} = \{\{1,2\},\{2,3\},\{3,4\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}$. We want to encode the secret image "ICALP 96". The four shares generated by a visual cryptography scheme for $\mathcal{A}$ are given in appendix. They look like random patterns and indeed no one of them gives any information, even to a very powerful machine, on the original image. To decrypt the secret image the reader should xerox each pattern on a separate transparency, stack together the transparencies associated to participants in any qualified set, and project the result with an overhead projector. If the transparencies are aligned carefully, then the reader will get the images showed in the remaining part of appendix.

This new cryptographic paradigm has been recently introduced by Naor and Shamir [8]. They analyzed the case of k out of n visual cryptography schemes in which the secret image is visible if and only if any k transparencies are stacked together. But the secret image is totally invisible if fewer than k transparencies are stacked together. A possible application of them is the following [8]. The 2 out of 2 visual cryptography scheme can be thought of as a private key cryptosystem. We encode the secret printed message into two randomly looking transparencies, one of the two image will be a printed page of ciphertext which can be sent by mail or fax, whereas the other printed transparency serves as a secret key. The original image is revealed by stacking together the two transparencies. This system is similar to the one time pad as each page of ciphertext is decoded by using a different transparency, but it is not required any cryptographic computation, the decoding is done by the human visual system.

Visual cryptography schemes with extended capabilities have been analyzed in [2]. The authors present a general technique to implement extended visual cryptography schemes which uses hypergraph colourings.

In this paper we extend the Naor and Shamir's model to *any* general access structure, where an access structure is a specification of all qualified subsets of participants. We propose two different techniques to construct visual cryptography schemes for any access structure. We analyze the structure of visual cryptography schemes and we prove bounds on the size of the image distributed to the participants in the scheme. We provide a novel technique to realize k out of n visual cryptography schemes. In particular we consider graph-based access structures, that is access structures in which any qualified set of participants contains at least an edge of a given graph whose vertices represent the participants of the scheme. Our constructions for 2 out of n visual cryptography schemes are the best possible with respect to pixel expansion and relative difference.

Due to the space limit all proofs have been omitted. The interested reader can find them in [1] along with other results on VCS and several examples.

2 The Model

Let $\mathcal{P}$ be a set of participants, a *monotone* access structure Γ on $\mathcal{P}$ is a subset $\Gamma \subseteq 2^{\mathcal{P}} \setminus \{\emptyset\}$, such that if $A \in \Gamma$ and $A \subseteq A' \subseteq \mathcal{P}$ then $A' \in \Gamma$.

The *closure* of Γ, denoted by $cl(\Gamma)$, is the set $\{C \mid B \in \Gamma \text{ and } B \subseteq C \subseteq \mathcal{P}\}$.

For a monotone access structure Γ we have $\Gamma = cl(\Gamma)$. All access structures considered in this paper are monotone.

Let Γ be an access structure, a set $C \in \Gamma$ is a *minimal* set of Γ if it does not contain any set in $\Gamma \setminus \{C\}$. A *basis* Γ_0 of Γ is the family of all minimal sets of Γ. In this paper we assume that $\mathcal{P} = \{1, \ldots, n\}$.

We will refer to a participant $P \in \mathcal{P}$ as an *essential* participant if there exists a set $X \subseteq \mathcal{P}$ such that $X \cup \{P\} \in \Gamma_0$. If a participant P is not essential then we can construct a visual cryptography scheme giving him nothing as share. In fact, a non-essential participant does not participate "actively" in the reconstruction of the image, that is the information he has is not needed by any set in $\mathcal{P}$ in order to recover the shared image. Therefore, any VCS handling non-essential participants can give to these participants nothing as share. In this paper we assume that the set of participants $\mathcal{P}$ consists only of essential participants.

For sets X and Y and for elements x and y, to avoid overburdening the notation, we often will write x for $\{x\}$, xy for $\{x, y\}$, xY for $\{x\} \cup Y$, and XY for $X \cup Y$.

We assume that the message consists of a collection of black and white pixels. Each pixel appears in n versions called *shares*, one for each transparency. Each share is a collection of m black and white subpixels. The resulting structure can be described by an $n \times m$ Boolean matrix $S = [s_{ij}]$ where $s_{ij} = 1$ iff the j-th subpixel in the i-th transparency is black. Therefore the grey level of the combined share, obtained by stacking the transparencies $i_1, \ldots, i_s$, is proportional to the Hamming weight $w(V)$ of the m-vector $V = OR(r_{i_1}, \ldots, r_{i_s})$ where $r_{i_1}, \ldots, r_{i_s}$ are the rows of S associated with the transparencies we stack. This grey level is interpreted by the visual system of the users as black or as white in according with some rule of contrast.

Definition 1. Let Γ be an access structure on a set of n participants. Two collections (multisets) of $n \times m$ boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ constitute a *visual cryptography scheme (Γ, m)-VCS* if there exist values $\alpha(m)$ and $\{t_X\}_{X \in \Gamma_0}$ satisfying:

1. *Any qualified set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_0$ can recover the shared image.* Formally, for any $S \in \mathcal{C}_0$, the "or" V of rows $i_1, i_2, \ldots, i_p$ satisfies $w(V) \leq t_X - \alpha(m) \cdot m$; whereas, for any $S \in \mathcal{C}_1$ it results that $w(V) \geq t_X$.
2. *Any non-qualified set $X = \{i_1, i_2, \ldots, i_p\} \notin \Gamma$ has no information on the shared image.*
   Formally, the two collections of $p \times m$ matrices $\mathcal{D}_t$, with $t \in \{0, 1\}$, obtained by restricting each $n \times m$ matrix in $\mathcal{C}_t$ to rows $i_1, i_2, \ldots, i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Each pixel of the original image will be encoded into n pixels each one consisting of m subpixels. To share a white/black pixel the dealer randomly chooses one of the matrices in $\mathcal{C}_0/\mathcal{C}_1$ and distributes row i to participant i. The chosen matrix defines the colour of the m subpixels in each one of the n transparencies. Observe that the size of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ does not need to be the same.

The first condition is related to the contrast of the image. It states that a qualified set of users, belonging to the basis of the access structure, stacking their transparencies can correctly recover the image shared by the dealer. The value $\alpha(m)$ is called *relative difference*, the number $\alpha(m) \cdot m$ is referred to as the *contrast* of the image, and the set $\{t_X\}_{X \in \Gamma_0}$ is called the *set of thresholds*. We want that $\alpha(m) \cdot m$ be as large as possible and at least 1 subpixel over the m subpixels, that is, $\alpha(m) \geq 1/m$. The second condition is called *security*, it implies that by inspecting the shares of a non-qualified subset of participants one cannot gain any advantage in deciding whether the shared pixel was white or black.

There are few differences between the model of visual cryptography we propose and the one presented by Naor and Shamir [8]. Our model is a generalization of the one proposed in [8] as to each set $X \in \Gamma_0$ it is associated a different threshold t_X and only sets in the basis can recover the shared image. If a set of participants $X \in \Gamma$ wants to recover the shared image, then they can consider only the shares of a set $X' \subseteq X$ such that $X' \in \Gamma_0$. Notice that with our definition it is not excluded that a set of participants $X \in \Gamma \backslash \Gamma_0$ stacking their transparencies does not get the original image. Visual cryptography schemes in which any set $X \in \Gamma$ satisfies Property 1 of the Definition 1 are called *strong*.

In this paper we consider only VCS in which the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ have the same size, i.e., $|\mathcal{C}_0| = |\mathcal{C}_1| = r$. Actually, this is not a restriction at all. Indeed, given an access structure Γ, we can obtain, from an arbitrary VCS for Γ, a VCS, having the same parameters m and $\alpha(m)$, with equally sized $\mathcal{C}_0$ and $\mathcal{C}_1$. Moreover, we do not consider access structures containing "isolated" participants, namely we suppose that for any $X \in \Gamma_0$ it holds that $|X| \geq 2$. If the access structure Γ contains some isolated participants, say $P_{i_1}, \ldots, P_{i_t}$, then we can always realize a VCS for Γ by "augmenting" a VCS Σ' for the access structure $\Gamma_0' = \Gamma_0 \setminus \left\{\{P_{i_1}\}, \ldots, \{P_{i_t}\}\right\}$. It is enough to add to any $M \in \mathcal{C}_0$ and any $M' \in \mathcal{C}_1$ new rows indexed by $i_1, \ldots, i_t$ whose entries are all equal to zero and to one, respectively.

2.1 Basis Matrices

Most of the constructions in this paper are realized using two $n \times m$ matrices, S^0 and S^1 called *basis matrices* satisfying the following definition.

Definition 2. Let Γ be an access structure on a set of n participants. A visual cryptography scheme (Γ, m)-VCS with relative difference $\alpha(m)$ and set of thresholds $\{t_X\}_{X \in \Gamma_0}$ is realized using the $n \times m$ basis matrices S^0 and S^1 if the following two conditions hold.

1. If $X = \{i_1, i_2, \ldots, i_p\}$ is a qualified set (i.e., $X \in \Gamma_0$), then: The "or" V of rows $i_1, i_2, \ldots, i_p$ of S^0 satisfies $w(V) \leq t_X - \alpha(m) \cdot m$; whereas, for S^1 it results that $w(V) \geq t_X$.
2. If $X = \{i_1, i_2, \ldots, i_p\}$ is not a qualified set (i.e., $X \notin \Gamma$) then: The two $p \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_p$ are equal up to a columns permutation.

The collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are obtained by permuting the columns of the corresponding matrix (S^0 for $\mathcal{C}_0$ and S^1 for $\mathcal{C}_1$) in all possible ways. Note that, in this case, the size of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ is the same and it is denoted by r. This technique has been introduced in [8]. The algorithm for the VCS based on the previous construction of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ has small memory requirements (it keeps only the basis matrices S^0 and S^1) and it is efficient (to choose a matrix in $\mathcal{C}_0$ ($\mathcal{C}_1$) it only generates a permutation of the columns of S^0 (S^1)).

3 An n Out of n Scheme

In this section we recall some of the results presented in [8] for *n out of n visual cryptography schemes* realizing the access structure $\Gamma = \{\mathcal{P}\}$, that is, the original message is visible if and only if all n transparencies are stacked together, but totally invisible if fewer than n transparencies are stacked together or analysed by any other method.

The construction of a general n out of n scheme is obtained by means of the construction of the basis matrices S^0 and S^1 defined as follows:
S^0 is the matrix whose columns are all the boolean n-vectors having an even number of 1; whereas, S^1 is the matrix whose columns are all the boolean n-vectors having an odd number of 1.

Lemma 3. ([8]) *The above scheme is a n out of n VCS with parameters $m = 2^{n-1}$, $\alpha(m) = 1/2^{n-1}$ and $r = 2^{n-1}!$.*

The scheme realized using the previous construction is optimal since in any n out of n visual cryptography scheme m has to be at least 2^{n-1} and $\alpha(m)$ can be at most $1/2^{n-1}$ (see [8]).

Let Γ be an access structure on a set $\mathcal{P}$ of participants. Given a subset of participants $\mathcal{P}' \subseteq \mathcal{P}$, we define the access structure *induced by $\mathcal{P}'$* as the family of sets $\Gamma[\mathcal{P}'] = \{X \in \Gamma : X \subseteq \mathcal{P}'\}$. The following lemma is immediate.

Lemma 4. *Let Γ be an access structure on a set $\mathcal{P}$ of participants and let Γ' be an induced structure of Γ. Let m' the minimum value for which there exists a (Γ', m')-VCS. For any (Γ, m)-VCS it has to be $m \geq m'$.*

4 General Constructions

In this section we will present two construction techniques to realize visual cryptography schemes for any access structure.

4.1 A Construction Using Cumulative Arrays

The first construction we consider is based on the *cumulative array* introduced in [10]. Let Γ be a monotone access structure on the set of participants $\mathcal{P} = \{1, 2, \ldots, n\}$. With Z_M we denote the collection of the maximal non-qualified sets of Γ. Hence,

$$Z_M = \{B \subseteq \mathcal{P} \mid B \notin \Gamma \text{ and } B \cup \{i\} \in \Gamma \text{ for all } \{i\} \in \mathcal{P} \setminus B\}.$$

A *cumulative map* (β, T) for the access structure Γ is a finite set T along with a mapping $\beta : \mathcal{P} \longrightarrow 2^T$ such that for $Q \subseteq \mathcal{P}$ we have that

$$\bigcup_{a \in Q} \beta(a) = T \Longleftrightarrow Q \in \Gamma.$$

We can realize a cumulative map (β, T) for any access structure Γ based on the collection of the maximal non-qualified sets $Z_M = \{S_1, \ldots, S_t\}$ as follows. Let $T = \{T_1, \ldots, T_t\}$ and for any $i \in \mathcal{P}$ let

$$\beta(i) = \{T_j \mid i \notin S_j, 1 \leq j \leq t\}. \tag{1}$$

It is easy to see that for any $X \in \Gamma$ we have $\bigcup_{i \in X} \beta(i) = T$; whereas any set $X \notin \Gamma$ will be missing a $T_j \in T$. From the previous cumulative mapping we can obtain a *cumulative array* CA as follows. A cumulative array CA is a $|\mathcal{P}| \times |T|$ boolean matrix such that $CA(i, j) = 1$ if and only if $i \notin S_j$.

At this point we can illustrate a technique to realize visual cryptography schemes for any access structure Γ. Our technique is based on the n out of n visual secret sharing scheme of Section 3. Let Z_M be set of the maximal non-qualified sets of Γ and let $t = |Z_M|$. Let CA be the cumulative array for Γ obtained using the cumulative map (1). Let $\hat{S}^0$ and $\hat{S}^1$ be the basis matrices for a t out of t visual cryptography scheme. The basis matrices S^0 and S^1 for a visual cryptography scheme for Γ can be constructed as follows. For any fixed i let $j_{i,1}, \ldots, j_{i,g_i}$ be the integers j such that $CA(i, j) = 1$. The i-th row of S^0 (S^1) consists of the *or* of the rows $j_{i,1}, \ldots, j_{i,g_i}$ of $\hat{S}^0$ $(\hat{S}^1)$.
Next theorem holds.

Theorem 5. *Let Γ be an access structure and let Z_M be the family of the maximal non-qualified sets of Γ. There exists a strong (Γ, m)-VCS with $m = 2^{|Z_M|-1}$ and $t_X = m$ for any $X \in \Gamma$.*

4.2 Constructing VCS from Smaller Schemes

In this section we present a construction for visual cryptography schemes using small schemes as building blocks in the construction of larger schemes.

Let Γ' and Γ'' be two access structures on a set of n participants $\mathcal{P}$. Suppose there exist a (Γ', m')-VCS and a (Γ'', m'')-VCS with basis matrices $S^{0,\Gamma'}$, $S^{1,\Gamma'}$ and $S^{0,\Gamma''}$, $S^{1,\Gamma''}$, respectively. We will show how to construct a VCS for the access structure $\Gamma = \Gamma' \cup \Gamma''$. From the matrices $S^{0,\Gamma'}$, $S^{1,\Gamma'}$, $S^{0,\Gamma''}$, and $S^{1,\Gamma''}$ we construct two pairs of matrices, $(\hat{S}^{0,\Gamma'}, \hat{S}^{1,\Gamma'})$ and $(\hat{S}^{0,\Gamma''}, \hat{S}^{1,\Gamma''})$, consisting of n rows as follows. Let us show how to construct $\hat{S}^{0,\Gamma'}$. For $i = 1, \ldots, n$, the i-th row of $\hat{S}^{0,\Gamma'}$ has all zeroes as entries if the participant i is not an essential participant of Γ'; otherwise, it is the row of $S^{0,\Gamma'}$ corresponding to participant i. The matrices $\hat{S}^{1,\Gamma'}$, $\hat{S}^{0,\Gamma'}$, and $\hat{S}^{1,\Gamma'}$ are constructed similarly. Finally, the basis matrices S^0 and S^1 for Γ will be realized concatenating the matrix $\hat{S}^{0,\Gamma'}$ with $\hat{S}^{0,\Gamma''}$ and the matrix $\hat{S}^{1,\Gamma'}$ with $\hat{S}^{1,\Gamma''}$, respectively (i.e., $S^0 = \hat{S}^{0,\Gamma'} \circ \hat{S}^{0,\Gamma''}$ and $S^1 = \hat{S}^{1,\Gamma'} \circ \hat{S}^{1,\Gamma''}$, where with $\circ$ we denote the operator "concatenation" of two matrices). Theorem 6 states that the scheme obtained using previous technique does realize a VCS.

Theorem 6. *Let Γ' and Γ'' be two access structures. For any (Γ', m')-VCS and (Γ'', m'')-VCS, both constructed using basis matrices, the previous construction gives a $(\Gamma' \cup \Gamma'', m' + m'')$-VCS. If the original VCS are strong so it is the resulting VCS.*

Next corollary is an immediate consequence of Theorem 6.

Corollary 7. *Let Γ be an access structure. If $\Gamma = \cup_{i=1}^{w} \Gamma_i$ and, for $i = 1, \ldots, w$, there exists a (Γ_i, m_i)-VCS constructed using basis matrices, then there exists a (Γ, m)-VCS, where $m = \sum_{i=1}^{w} m_i$. If the original VCS are strong so it is the resulting VCS.*

From Lemma 3 and Corollary 7 the following theorem holds.

Theorem 8. *Let Γ be an access structure. There exists a strong (Γ, m)-VCS where* $m = \displaystyle\sum_{X \in \Gamma_0} 2^{|X|-1}$.

Previous theorem states a general result on the existence of VCS for any access structure Γ. For special classes of access structures it is possible to achieve a smaller value of m as we will show in Section 6 for k out of n VCS and in Section 7 for graph-based access structures.

5 On the Structure of VCS

In this section we provide some useful properties of VCS. First, we show how to construct VCS for any non-connected access structure using VCS for its connected parts. Then, we prove that any matrix M in the collection $\mathcal{C}_0 \cup \mathcal{C}_1$ has to contain some predefined patterns (sub-matrices).

Non-Connected Access Structures An access structure Γ on a set of participants $\mathcal{P}$ is *connected* if there is no partition of $\mathcal{P}$ in two sets $\mathcal{P}'$ and $\mathcal{P}''$ such that $\Gamma_0 \subseteq 2^{\mathcal{P}'} \cup 2^{\mathcal{P}''}$. If an access structure Γ is not connected, then we can realize a VCS for Γ simply by constructing VCS for its connected parts and then by putting together the schemes in a suitable way as stated in the next theorem.

Theorem 9. *Let Γ' and Γ'' be two access structures on disjoint sets of participants $\mathcal{P}'$ and $\mathcal{P}''$, respectively. If there exist a (Γ', m')-VCS and a (Γ'', m'')-VCS, then there is a $(\Gamma' \cup \Gamma'', m)$-VCS, where $m = \max\{m', m''\}$.*

Unavoidable Patterns Let M be a matrix in the collection $\mathcal{C}_0 \cup \mathcal{C}_1$ of a (Γ, m)-VCS for the access structure Γ on a set of participants $\mathcal{P}$. For $X \subseteq \mathcal{P}$, M_X denotes the m-vector obtained considering the *or* of the vectors corresponding to participants in X; whereas $M[X]$ denotes the $|X| \times m$ matrix obtained from M by considering only the rows corresponding to participants in X.

Lemma 10. *Let X and Y be two non-empty subsets of participants and let Γ be an access structure. If $XY \in \Gamma_0$, then in any (Γ, m)-VCS, for any matrix $M \in \mathcal{C}_1$ it holds that*

$$w(M_{XY}) - w(M_X) \geq \alpha(m) \cdot m.$$

The matrices in $\mathcal{C}_0 \cup \mathcal{C}_1$ have to contain some predefined patterns referred to as *unavoidable patterns*. For instance, for any $X \in \Gamma_0$ and any matrix $M \in \mathcal{C}_1$, the matrix $M[X]$, for $i = 1, \ldots, |X|$, contains at least $\alpha(m) \cdot m$ columns with '1' in the i-th position and all zeroes in the other entries. This is an immediate consequence of Lemma 10. Indeed, by considering $X = Y \cup \{i\}$ we get $w(M_{Y \cup \{i\}}) - w(M_Y) \geq \alpha(m) \cdot m$. Therefore, there must be at least $\alpha(m) \cdot m$ columns in $M[X]$ with '1' in the row i and all zeroes in the other entries. Another unavoidable pattern contained in any matrix $M \in \mathcal{C}_0$ is the following: For any $X \in \Gamma_0$ the matrix $M[X]$ contains at least $\alpha(m) \cdot m$ columns with entries all equal to '0'. In fact from Property 1. of Definition 1 we have $w(M_X) \leq t_X - \alpha(m) \cdot m \leq m - \alpha(m) \cdot m$. Next corollaries are immediate consequences of the unavoidable patterns.

Corollary 11. *Let Γ be an access structure on a set of participants $\mathcal{P}$. For any essential participant $i \in \mathcal{P}$, in any (Γ, m)-VCS, for any matrix $M \in \mathcal{C}_0 \cup \mathcal{C}_1$ it holds that $w(M_i) \geq \alpha(m) \cdot m$.*

Corollary 12. *In any (Γ, m)-VCS where $\Gamma \neq \mathcal{P}$ it holds that $m \geq 2$.*

Corollary 13. *For any $X \in \Gamma_0$ we have $t_X \geq |X| \cdot \alpha(m) \cdot m$.*

Another consequence of the unavoidable patterns is that for the access structures based on complete graphs (i.e., access structures such that $\Gamma_0 = \{\{i, j\} : i, j \in \mathcal{P}\}$) the rows of any matrix $M \in \mathcal{C}_1$ of a VCS represent a Sperner family (see for example [6]). In fact, let $M \in \mathcal{C}_1$ be an $n \times m$ boolean matrix and let $G = \{g_1, \ldots, g_m\}$ be a ground set. For $i = 1, \ldots, n$, row i of M represents the subset $A_i = \{g_w :$ the entry (i, w) of M is equal to $1\}$ of G. Since any two rows of M contain the patterns $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, then the sets $A_1, \ldots, A_n$ constitute a Sperner family in the ground set G. Therefore, the rows of the matrix M represent a Sperner family. This will be exploited in Theorem 19 and in Section 7. The following basis matrices represent a VCS for the access structure based on the complete graph with 6 vertices. This scheme is constructed from a Sperner family in a ground set containing four elements.

$$S^0 = \begin{bmatrix} 1100 \\ 1100 \\ 1100 \\ 1100 \\ 1100 \\ 1100 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 1010 \\ 1001 \\ 1100 \\ 0110 \\ 0101 \\ 0011 \end{bmatrix}.$$

Next lemma states the existence of other unavoidable patterns in any matrix in the collections $\mathcal{C}_0$ and $\mathcal{C}_1$. Basically, it says that for any $Y \notin \Gamma$ and for any $M \in \mathcal{C}_0 \cup \mathcal{C}_1$, the matrix $M[Y]$ contains at least $\alpha(m) \cdot m$ columns whose entries are all equal to zero.

Lemma 14. *Let Y and Z two nonempty subsets of participants such that $ZY \in \Gamma_0$. In any (Γ, m)-VCS, for any matrix $M \in \mathcal{C}_0 \cup \mathcal{C}_1$ it holds that*

$$w(M_Y) \leq \min\{t_X : Y \subset X,\ X \in \Gamma_0\} - \alpha(m) \cdot m.$$

Next lemma shows the existence of unavoidable patterns in any matrix $M \in \mathcal{C}_0$ of any strong VCS.

Lemma 15. *Let Γ be an access structure on a set $\mathcal{P}$ of participants. In any strong (Γ, m)-VCS any matrix $M \in \mathcal{C}_0$ has at least $\alpha(m) \cdot m$ columns whose entries are all equal to zero.*

Next theorem, based on the existence of the unavoidable patterns, provides a characterization of VCS having $m = 2$.

Theorem 16. *Let Γ be a connected access structure. If there exists a $(\Gamma, 2)$-VCS, then Γ_0 is the edge-set of a complete bipartite graph.*

6 A k Out of n Scheme

A k out of n visual cryptography scheme (also called (k, n)-threshold scheme) realizes the access structure:

$$\{B \subseteq \mathcal{P} : |B| \geq k\}.$$

For k out of n schemes the original message is visible if any k of n participants stack their transparencies, but totally invisible if fewer than k transparencies are stacked together or analysed by any other method.

We can construct k out of n visual cryptography schemes by using the two techniques described in Sections 4.1 and 4.2. By using the technique based on cumulative arrays we obtain a strong k out of n VCS in which $m = 2^{\binom{n}{k-1}-1}$ and $t_X = m$ for any set X of cardinality k; whereas by using the technique of Section 4.2 we obtain a strong k out of n VCS in which $m = \binom{n}{k} \cdot 2^{k-1}$ and t_X has the same value for any set X of cardinality k.

In the following we describe a method to construct k out of n VCS achieving better results, in terms of the size of the shares, than the techniques described in Sections 4.1 and 4.2. The method we introduce is based on *perfect hashing* [5, 7, 3].

Definition 17. A *starting matrix* $SM(n,l,k)$ is a $n \times l$ matrix whose entries are elements of a set $\{a_1, \ldots, a_k\}$, with the property that, for any subset of k rows, there exists at least one column such that the entries in the k given rows of that column are all distinct.

Given a matrix $SM(n,l,k)$ we can construct a k out of n VCS as follows: The $n \times (l \cdot 2^{k-1})$ basis matrices S^0 and S^1 are constructed by replacing the symbols $a_1, \ldots, a_k$, respectively, with the 1-st,…, k-th rows of the corresponding basis matrices of the k out of k VCS described in Section 3. The scheme obtained is a k out of n VCS as the following theorem states.

Theorem 18. *If there exists a $SM(n,l,k)$ then there exists a strong k out of n VCS with $m = l \cdot 2^{k-1}$.*

The SM matrix is a representation of a *Perfect Hash Family* (PHF). Fredman and Komlós [5] proved that for any PHF it holds that $l = \Omega(k^{k-1}/k!) \log n$. They also proved the weaker but simpler bound $l = \Omega(1/\log k) \log n$. Melhorn [7] proved that there exist PHFs with $l = O(ke^k) \log n$. In [3] it has been provided a recursive construction for PHFs with $l = O\left((\log n)^{\log(\binom{k}{2}+1)}\right)$.

Naor and Shamir [8] showed that there exist k out of n visual cryptography schemes with $m = 2^{O(k \log k)} \cdot \log n$. Our construction produce a smaller value of m than their construction, but this has been achieved by relaxing the condition that t_X are equal as required in [8].

Next theorem provides a lower bound on m for any k out of n visual cryptography scheme.

Theorem 19. *In any k out of n visual cryptography scheme it results that*

$$\binom{n}{k-1} \leq \binom{m}{\lfloor m/2 \rfloor}.$$

Since $\binom{m}{\lfloor m/2 \rfloor} \leq 2^m$ and $\binom{n}{k-1} \geq (\frac{n}{k-1})^{k-1}$ we have that in any k out of n visual cryptography scheme $m = \Omega(k \log(n/k))$.

7 VCS for Graph Access Structures

In this section we present some bounds on the size of the shares for graph-based access structures. A graph-based access structure is an access structure which is the closure of the edge set of a given graph, that is, an access structure for which the set of participants can be identified with the vertex set $V(G)$ of a graph $G = (V(G), E(G))$, and the sets of participants qualified to reconstruct the secret image are precisely those containing an edge of G.

We first recall some terminology from graph theory. Given a graph $G = (V(G), E(G))$ a *vertex cover* of G is a subset of vertices $A \subseteq V(G)$ such that every edge in $E(G)$ is incident with at least one vertex in A. The *complete graph* K_n is the graph on n vertices in which any two vertices are joined by an edge. The *complete multipartite graph* $K_{a_1,a_2,\ldots,a_n}$ is a graph on $\sum_{i=1}^{n} a_i$ vertices, in which the vertex set is partitioned into subsets of size a_i $(1 \leq i \leq n)$ called *parts*, such that vw is an edge if and only if v and w are in different parts. An alternative way to characterize a complete multipartite graph is to say that the complementary graph is a vertex-disjoint union of cliques. Note that the complete graph K_n can be thought of as a complete multipartite graph with n parts of size 1.

Exploiting the construction used in Theorem 6 we can prove the following theorem.

Theorem 20. *Suppose G is a graph with a vertex cover of size v and let $\Gamma_0 = E(G)$. Then, there exists a $(\Gamma, 2v)$-VCS.*

The following result can be obtained applying Theorem 19.

Corollary 21. *Let $\Gamma_0 = E(K_n)$. There exists a (Γ, m)-VCS if and only if $n \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

A modification of Corollary 21, using the well-known "splitting technique" from secret sharing schemes, together with Lemma 4, can be used to prove the following result for complete multipartite graphs.

Theorem 22. *Let $\Gamma_0 = E(K_{a_1,\ldots,a_n})$. There exists a (Γ, m)-VCS if and only if $n \leq \binom{m}{\lfloor \frac{m}{2} \rfloor}$.*

Let $\Gamma = cl(E(K_n))$. Corollary 21 proves a lower bound on the value of m for a (Γ, m)-VCS which is met with equality when the VCS for Γ is constructed from a Sperner family in a ground set of m elements. In such a scheme we have $\alpha(m) = 1/m$. If we are interested in realizing schemes achieving a greater relative difference, then we can use the following construction. The basis matrix S^1 is realized by considering all the columns of weight $\lfloor n/2 \rfloor$. Hence, $m = \binom{n}{\lfloor n/2 \rfloor}$. It is easy to see that any row in S^1 has weight equal to $\binom{n-1}{\lfloor n/2 \rfloor - 1}$. The basis matrix S^0 is realized by considering n equal rows of weight $\binom{n-1}{\lfloor n/2 \rfloor - 1}$. In such a scheme we have $\alpha(m) = (\lfloor n/2 \rfloor \lceil n/2 \rceil)/(n^2 - n)$. This is the best possible value for the relative difference as stated by the following theorem.

Theorem 23. *Let $\Gamma_0 = E(K_n)$. In any (Γ, m)-VCS it holds that*

$$\alpha(m) \leq \frac{\lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil}{n(n-1)}.$$

It is possible to construct schemes with a smallest pixel expansion achieving the bound provided by previous theorem. These schemes are based on Hadamard matrices and designs. In such schemes we have that $m = n$ and we will prove in the final version of this paper that the construction from the Hadamard matrix achieves the smallest possible m (for the given maximum possible $\alpha(m)$).

Using the splitting technique together with Lemma 4 we obtain that the bound provided by Theorem 23 holds also when $\Gamma_0 = E(K_{a_1,\ldots,a_n})$.

Acknowledgements We would like to express our gratitude to Ugo Vaccaro for illuminating discussions. Many thanks go to Carmine Di Marino who implemented the techniques presented in this paper and provided us with the images depicted in the appendix.

References

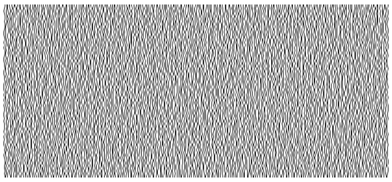
1. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Visual Cryptography for General Access Structures*. Available from *ECCC*, Electronic Colloquium on Computational Complexity (TR96–012), via WWW using `http://www.eccc.uni-trier.de/eccc/`.
2. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Extended Schemes for Visual Cryptography*, preprint, 1995.
3. M. Atici, S. S. Magliveras, D. R. Stinson, and W.-D. Wei, *Some Recursive Constructions for Perfect Hash Families*, Technical Report UNL, Univ. of Nebraska-Lincoln, June 1995.
4. C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, *Graph Decomposition and Secret Sharing Schemes*, Journal of Cryptology, Vol. 8, (1995), pp. 39-64.
5. M. L. Fredman and J. Komlós, *On the Size of Separating System and Families of Perfect Hash Functions*, SIAM J. Alg. Disc. Meth., Vol 5, No 1, March 1984.
6. J. H. van Lint and R. M. Wilson, A Course in Combinatorics, Cambridge University Press, (1992).
7. K. Melhorn, *On the Program Size of Perfect and Universal Hash Functions*, in Proc. of 23rd Annual IEEE Symposium on Foundation of Computer Science, pp. 170–175, 1982.
8. M. Naor and A. Shamir, *Visual Cryptography*, in "Advances in Cryptology – Eurocrypt '94", A. De Santis Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 1–12, 1995.
9. P. Elias, *Zero Error Capacity Under List Decoding*, IEEE Trans. Inform. Theory, Vol. 34, 1988.
10. G. J. Simmons, W. Jackson, and K. Martin, *The Geometry of Shared Secret Schemes,* Bulletin of the ICA, 1:71–88, 1991.
11. D. R. Stinson, *Decomposition Constructions for Secret Sharing Schemes*, IEEE Trans. Inform. Theory, Vol. 40, pp. 118–125, 1994.

Visual Cryptography for "ICALP 96"

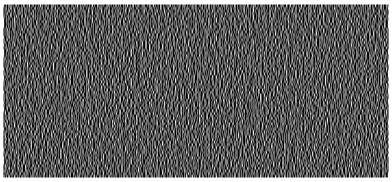
In this appendix an example of the secret image, the shares corresponding to single participants, and few groups of participants are depicted. The access structure is $\{\{1,2\},\{2,3\},\{3,4\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}$.

Secret Image

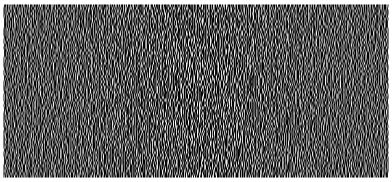
Share of participant 1



Share of participant 2



Share of participant 3



Share of participant 4

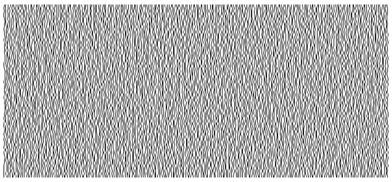


Image of participants 1 and 2

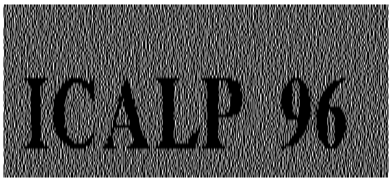


Image of participants 2 and 3

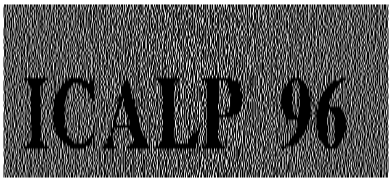


Image of participants 3 and 4

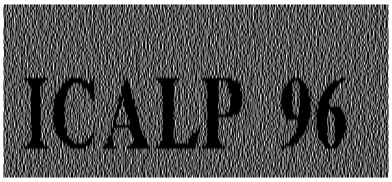


Image of participants 1 and 3